Sveriges cybersäkerhet

ZOURKAN

MR.YOUSSEF ZOURKANE

Boktitel: Skydd i den digitala eran: NIS2 och Sveriges cybersäkerhetsresa

Undertitel: Hur EU:s direktiv formar nationell säkerhet i en tid av cyberhot

Författare: Grok (med inspiration från xAI:s mission att främja kunskap)

Introduktion: En ny era för cybersäkerhet

I oktober 2024 skakades Östersjöregionen av en serie mystiska incidenter. Två undervattenskablar, avgörande för internettrafiken mellan Sverige och dess grannar, skadades under oklara omständigheter. Misstankarna riktades snabbt mot sabotage, och Rysslands skugga föll tungt över analyserna. Samtidigt drabbades flera nordiska banker och offentliga institutioner av omfattande överbelastningsattacker, som lamslog digitala tjänster och väckte frågor om Sveriges beredskap. Dessa händelser, som inträffade mitt under Sveriges första år som Natomedlem, var en brutal påminnelse om en ny verklighet: cybersäkerhet är inte längre en teknisk detalj – det är en grundpelare i nationell säkerhet.

I denna tid av osäkerhet träder NIS2-direktivet (Directive (EU) 2022/2555) fram som en av de mest ambitiösa satsningarna för att skydda Europas och Sveriges digitala infrastruktur. Som efterföljare till det första NIS-direktivet från 2016 markerar NIS2 en ny era, där samhällsviktiga tjänster – från energibolag och sjukhus till kommuner och molntjänster – sätts under strängare krav för att motstå cyberhot. Direktivet är inte bara en teknisk reform; det är en strategisk nödvändighet i en värld där statliga aktörer, organiserade brottsgrupper och ensamma hackare kan orsaka kaos med några få klick.

Sverige, som ett av världens mest digitaliserade länder, står i centrum för denna omvandling. Med en ekonomi som bygger på innovation, en kritisk infrastruktur som är djupt uppkopplad, och en geopolitisk position som Natomedlem i en spänd Östersjöregion, är Sveriges sårbarhet lika stor som dess potential. NIS2-direktivet tvingar Sverige att konfrontera dessa utmaningar: Hur skyddar vi våra kommuner från ransomware? Hur säkrar vi leverantörskedjor i en globaliserad värld? Och hur balanserar vi säkerhet med de demokratiska värderingar som definierar oss?

Denna bok, *Skydd i den digitala eran: NIS2 och Sveriges cybersäkerhetsresa*, är en djupdykning i NIS2-direktivets värld och dess betydelse för Sverige. Vi utforskar direktivets tekniska detaljer, dess implementering i svensk lagstiftning, och de praktiska utmaningar som kommuner, företag och myndigheter står inför. Men vi går också bortom paragraferna för att reflektera över de större frågorna: Hur bygger vi ett resilient samhälle i en tid av hybridhot? Vad innebär det att vara en ledare inom cybersäkerhet? Och hur kan vi engagera medborgarna i en kamp som inte bara handlar om teknik, utan om vår gemensamma framtid?

Boken är skriven för beslutsfattare, IT-experter, studenter och alla som vill förstå hur Sverige navigerar i denna nya era. Genom fallstudier, analyser och framåtblickande förslag erbjuder vi en färdplan för att inte bara uppfylla NIS2:s krav, utan att använda dem som en språngbräda för att stärka Sveriges säkerhet och konkurrenskraft. För i en värld där hoten är osynliga men konsekvenserna högst verkliga, är cybersäkerhet inte bara en fråga om skydd – det är en fråga om överlevnad.

Välkommen till resan.

Kapitel 1: Cybersäkerhet i en osäker värld

En värld under attack

Den 15 oktober 2024, strax efter midnatt, försvann plötsligt internetförbindelsen mellan Sverige och Litauen. En undervattenskabel i Östersjön, en av de digitala artärer som förbinder regionen, hade skadats. Bara dagar senare rapporterades en liknande incident med en annan kabel mellan Finland och Estland. Myndigheter i Sverige och dess grannländer pekade snabbt på sabotage, och misstankarna riktades mot Ryssland, vars hybridkrigföring alltmer inkluderar attacker mot kritisk infrastruktur. Samtidigt drabbades flera svenska banker och kommunala tjänster av en våg av överbelastningsattacker (DDoS), som tillfälligt lamslog deras digitala plattformar. För medborgare som försökte betala räkningar eller boka läkartider var det en frustrerande påminnelse om hur sårbart vårt moderna samhälle är.

Dessa händelser är inte isolerade. De är symtom på en ny era där cybersäkerhet inte längre är en teknisk sidnot, utan en central del av nationell och global säkerhet. Från statliga aktörer som Ryssland och Kina till organiserade kriminella grupper och ensamma hackare – hoten är många, och deras konsekvenser är djupgående. En enda lyckad attack kan störa elförsörjning, sabotera sjukvårdssystem eller underminera förtroendet för demokratiska institutioner. För Sverige, ett land som är både högteknologiskt och geopolitiskt exponerat, är insatserna högre än någonsin. Detta kapitel tar oss till hjärtat av den globala och svenska cybersäkerhetshotbilden år 2025. Vi utforskar varför Sverige är ett attraktivt mål, hur hoten har utvecklats och varför NIS2-direktivet har blivit en nödvändig respons. Genom att förstå dessa dynamiker kan vi bättre uppskatta den resa som Sverige står inför – en resa som handlar om att skydda inte bara våra system, utan själva fundamentet för vårt samhälle.

Den globala hotbilden: En mångfacetterad fiende

Cybersäkerhetshoten 2025 är lika varierade som de är farliga. Säkerhetspolisen, Försvarsmakten och internationella organisationer som NATO och EU identifierar flera nyckelaktörer och metoder:

- **Statliga aktörer: Främmande makter, särskilt Ryssland, Kina och Iran, använder cyberattacker som ett verktyg för spionage, sabotage och geopolitisk påverkan. Rysslands invasion av Ukraina 2022 markerade en vändpunkt, där cyberattacker blev en integrerad del av krigföringen. Grupper som Sandworm, kopplade till ryska underrättelsetjänster, har attackerat allt från ukrainska elnät till västerländska institutioner. I Sverige har Säkerhetspolisen varnat för att statliga aktörer riktar sig mot forskning,**

försvarsindustri och kritisk infrastruktur, ofta genom avancerade metoder som spearphishing och nolldagsexploateringar.

- Organiserad brottslighet: Kriminella grupper driver en blomstrande industri av ransomware, där de låser organisationers system och kräver lösensummor. Enligt en rapport från Myndigheten för samhällsskydd och beredskap (MSB) drabbades över 30 svenska kommuner och regioner av ransomware mellan 2020 och 2024, med kostnader i hundratals miljoner kronor. Dessa attacker är inte bara ekonomiska; de kan också destabilisera samhället genom att störa vård eller skolor.
- Hybridhot: Cyberattacker kombineras ofta med desinformation och fysiska handlingar för att skapa kaos. Under hösten 2024 rapporterades försök att sprida falska nyheter om svenska myndigheter parallellt med DDoS-attacker, sannolikt i syfte att undergräva förtroendet för regeringen. Sådana hybridhot är särskilt svåra att motverka, eftersom de kräver samordning mellan cybersäkerhet, underrättelsetjänst och kommunikation.
- Nya teknologier, nya risker: Utvecklingen av artificiell intelligens (AI) och kvantdatorer öppnar både möjligheter och hot. AI-drivna attacker, som automatiserade phishing-kampanjer, blir alltmer sofistikerade, medan kvantdatorer i framtiden kan knäcka dagens krypteringsmetoder. Samtidigt gör sakernas internet (IoT) och 5G-nätverk samhället mer uppkopplat – och därmed mer sårbart.

Den globala hotbilden präglas också av en asymmetri: en enskild aktör med begränsade resurser kan orsaka oproportionerlig skada. En tonåring med en laptop kan, med rätt verktyg, störa en hel kommuns verksamhet. Detta gör cybersäkerhet till en unik utmaning, där traditionella försvarsmetoder inte räcker.

Sverige i skottlinjen

Sverige är särskilt utsatt av flera skäl. Som ett av världens mest digitaliserade länder är vi beroende av teknologi i alla delar av samhället. Över 90 % av svenskarna använder internet dagligen, och sektorer som finans, vård och energi är djupt integrerade med digitala system. Denna uppkoppling är en styrka, men också en akilleshäl. En attack mot en enda nod – som en eldistributör eller ett sjukhus – kan få kaskadeffekter som påverkar miljontals människor.

Sveriges geopolitiska position förstärker riskerna. Som nybliven Natomedlem (sedan mars 2024) är Sverige en del av västvärldens försvarsallians, vilket gör landet till ett mål för aktörer som Ryssland. Östersjöregionen, där Sverige är en nyckelspelare, är en hotspot för spänningar, särskilt efter incidenter som de skadade

undervattenskablarna. Dessutom gör Sveriges starka stöd till Ukraina – inklusive miljarder i militärt bistånd – landet till en måltavla för ryska hybridattacker.
Kommuner och småföretag är särskilt sårbara. En rapport från MSB 2024 visar att över hälften av Sveriges kommuner saknar grundläggande cybersäkerhetsåtgärder, som multifaktorautentisering eller regelbundna säkerhetsuppdateringar. Småföretag, som ofta levererar tjänster till större aktörer, är också svaga länkar i leverantörskedjan. Ett exempel är en attack mot en svensk underleverantör till försvarsindustrin 2023, där känsliga data läckte till en utländsk aktör.
Sveriges höga teknologiska nivå gör också landet attraktivt för spionage. Universitet, forskningsinstitut och techföretag är mål för aktörer som vill stjäla innovationer inom AI, bioteknik och försvarsteknologi. Säkerhetspolisen har rapporterat en ökning av försök till cyberintrång mot akademiska institutioner, ofta maskerade som legitima samarbeten.

Från NIS1 till NIS2: En historisk nödvändighet

För att förstå varför NIS2-direktivet är så viktigt måste vi blicka tillbaka på dess föregångare, NIS1-direktivet (Directive (EU) 2016/1148). Antaget 2016 var NIS1 EU:s första försök att harmonisera cybersäkerhet i medlemsstaterna. Det införde krav på säkerhetsåtgärder för operatörer av samhällsviktiga tjänster (t.ex. energi och transport) och digitala tjänsteleverantörer (t.ex. molntjänster). Medlemsstaterna ålades att utse nationella myndigheter och etablera CSIRT (Computer Security Incident Response Teams) för att hantera incidenter.
NIS1 var ett steg framåt, men det hade brister. Implementeringen varierade kraftigt mellan länder, vilket skapade luckor i EU:s cybersäkerhet. Många sektorer, som livsmedelsproduktion och kommunal förvaltning, omfattades inte, trots deras samhällsviktiga roll. Sanktionerna för bristande efterlevnad var svaga, och samarbetet mellan medlemsstater var ofta ineffektivt. Dessutom hann hotbilden förändras dramatiskt mellan 2016 och 2020, drivet av händelser som Rysslands cyberattacker mot Ukraina och den ökande frekvensen av ransomware.
Redan 2020 insåg EU att en uppdatering var nödvändig. NIS2-direktivet, som antogs i december 2022 och trädde i kraft i januari 2023, är resultatet av denna insikt. Det utökar tillämpningsområdet till fler sektorer, skärper säkerhetskraven, inför strängare sanktioner och betonar internationellt samarbete. För Sverige, som redan kämpade med att stärka sitt cyberförsvar, blev NIS2 en katalysator för förändring – men också en utmaning, med tanke på de resurser och den samordning som krävs.

Varför NIS2 är avgörande för Sverige

NIS2-direktivet är mer än en byråkratisk reform; det är en strategisk nödvändighet för Sverige. Genom att tvinga fram robusta säkerhetsåtgärder för samhällsviktiga tjänster – från sjukhus och elbolag till kommuner och molntjänster – bidrar det till att minska sårbarheter i ett alltmer uppkopplat samhälle. Direktivet adresserar också Sveriges specifika utmaningar:

- **Skydd av kritisk infrastruktur: Händelser som kabelbrotten 2024 visar att Sverige måste stärka skyddet av fysisk och digital infrastruktur. NIS2:s krav på riskanalyser och incidentrapportering är ett steg i rätt riktning.**
- **Stärkt motståndskraft i kommuner: Genom att klassificera kommuner som väsentliga enheter tvingas de prioritera cybersäkerhet, vilket kan minska risken för attacker som den mot Västhamn (se introduktionen till vår bok).**
- **Internationellt samarbete: Som Natomedlem och EU-land drar Sverige nytta av NIS2:s fokus på informationsdelning och samordning, vilket är avgörande för att motverka gränsöverskridande hot.**
- **Ekonomisk konkurrenskraft: Genom att uppfylla NIS2:s krav kan svenska företag stärka sitt rykte som pålitliga aktörer på den globala marknaden, särskilt inom tech och innovation.**

Men NIS2 är inte utan utmaningar. Den korta tidsramen för implementering (senast oktober 2024 för nationell lagstiftning, med full effekt 2025/2026), bristen på cybersäkerhetsexperter och de ekonomiska bördorna för kommuner och småföretag är betydande hinder. Dessa frågor kommer att utforskas i senare kapitel, men redan nu är det tydligt att NIS2 markerar början på en ny fas i Sveriges cybersäkerhetsresa.

Mot en resilient framtid

Cybersäkerhet är inte längre en fråga för IT-avdelningar – det är en fråga för hela samhället. I en värld där hoten är osynliga men konsekvenserna högst verkliga, står Sverige inför ett val: att reagera på attacker när de inträffar, eller att proaktivt bygga en motståndskraft som kan stå emot framtidens stormar. NIS2-direktivet är en färdplan för det senare, men dess framgång beror på hur väl Sverige kan mobilisera resurser, samordna aktörer och engagera medborgarna.

Detta kapitel har gett en glimt av den värld vi lever i – en värld där cyberhot är en del av vardagen, men också en värld där vi har verktygen att kämpa tillbaka. I nästa kapitel dyker vi djupare in i NIS2-direktivet självt: dess struktur, krav och ambitioner. För att förstå Sveriges framtid måste vi först förstå det ramverk som ska forma den.

Kapitel 2: NIS2-direktivet: En djupdykning

En blueprint för säkerhet

I hjärtat av Europas svar på den växande cyberhotbilden ligger NIS2-direktivet – ett ambitiöst ramverk som syftar till att skydda samhällsviktiga tjänster och stärka unionens digitala motståndskraft. Officiellt känt som *Directive (EU) 2022/2555*, antogs NIS2 i december 2022 och markerar en betydande uppgradering från sitt föregångardirektiv, NIS1, som introducerades 2016. Där NIS1 var en pionjär i att harmonisera cybersäkerhet inom EU, är NIS2 en mer omfattande och tvingande respons på en värld där cyberattacker har blivit både vanligare och mer destruktiva. För Sverige, ett land där digital infrastruktur är livsnerven i ekonomi och samhälle, är NIS2 inte bara en EU-förordning – det är en strategisk nödvändighet. Direktivet omfattar allt från elnät och sjukhus till kommunala tjänster och molnleverantörer, och det ställer krav som kommer att forma hur dessa aktörer skyddar sig mot hot som ransomware, statligt sponsrat spionage och sabotage. Men vad innebär NIS2 i praktiken? Hur skiljer det sig från NIS1? Och hur passar det in i EU:s bredare vision för cybersäkerhet?

Detta kapitel tar oss in i NIS2-direktivets kärna. Vi dissekerar dess struktur, utforskar dess krav och analyserar dess ambitioner. Genom konkreta exempel från sektorer som energi, hälso- och sjukvård och digital infrastruktur visar vi hur direktivet kommer att påverka Sverige och varför det är en milstolpe i kampen för ett säkrare digitalt samhälle.

Strukturen i NIS2: En översikt

NIS2-direktivet är uppbyggt för att adressera de brister som identifierades i NIS1 och möta den snabbt föränderliga hotbilden. Det introducerar en rad nya krav och mekanismer, organiserade kring fem huvudsakliga pelare: tillämpningsområde, säkerhetsåtgärder, incidentrapportering, tillsyn och sanktioner, samt internationellt samarbete. Här är en detaljerad genomgång:

- **Utökat tillämpningsområde**
  NIS2 utvidgar betydligt vilka organisationer som omfattas jämfört med NIS1. Organisationer delas in i två kategorier:
  - **Väsentliga enheter (*essential entities*): Stora aktörer inom sektorer som är kritiska för samhällets funktion, såsom energi, transport, hälso- och sjukvård, finans, vattenförsörjning, digital infrastruktur (t.ex. molntjänster och datacenter) och offentlig förvaltning. Exempel i Sverige inkluderar Vattenfall (energi), Region Stockholm (hälso- och sjukvård) och Telia (telekom).**

- **Viktiga enheter (*important entities*): Mindre aktörer inom sektorer som livsmedelsproduktion, avfallshantering, posttjänster, kemiindustri och digitala tjänster (t.ex. sociala medieplattformar). Ett exempel är en regional livsmedelsproducent eller en mindre kommunal avfallsoperatör. Till skillnad från NIS1 baseras klassificeringen inte enbart på organisationens storlek utan också på dess samhällsviktiga roll. Organisationer med fler än 50 anställda eller en årsomsättning över 10 miljoner euro omfattas generellt, men vissa verksamheter – som små sjukhus eller kommuner – kan klassas som väsentliga oavsett storlek. Nya sektorer, som rymdteknik och avfallshantering, har lagts till för att reflektera moderna sårbarheter.**

- **Skärpta säkerhetskrav**
  NIS2 ställer stränga krav på organisationer att implementera riskbaserade säkerhetsåtgärder. Dessa inkluderar:
  - **Riskanalyser: Regelbundna bedömningar av cybersäkerhetsrisker, inklusive hot mot leverantörskedjor.**
  - **Säkerhetspolicyer: Utveckling av interna riktlinjer för att hantera cyberhot.**
  - **Incidenthantering: Planer för att snabbt identifiera, mildra och återhämta sig från attacker.**
  - **Tekniska skyddsåtgärder: Användning av kryptering, multifaktorautentisering och brandväggar.**
  - **Utbildning: Obligatorisk cybersäkerhetsutbildning för anställda, från ledning till frontlinjepersonal.**
  - **Leverantörskedjesäkerhet: Organisationer måste säkerställa att tredjepartsleverantörer (t.ex. molntjänster eller IT-konsulter) uppfyller samma säkerhetsstandarder. Ett exempel är ett sjukhus som Region Skåne, som nu måste granska säkerheten hos sina medicinska journalsystemleverantörer och utbilda personal i att identifiera phishing-försök.**

- **Incidentrapportering**
  NIS2 inför strikta regler för rapportering av cyberincidenter. Organisationer måste:
  - **Rapportera betydande incidenter till nationella myndigheter inom 24 timmar (initial rapport).**

- **Lämna en detaljerad rapport inom 72 timmar.**
- **Skicka en slutrapport inom en månad, inklusive orsaksanalys och åtgärder. En betydande incident definieras som en händelse som orsakar eller riskerar att orsaka betydande skada, t.ex. ett dataintrång som exponerar patientdata eller en attack som stör elförsörjningen. I Sverige kommer Myndigheten för samhällsskydd och beredskap (MSB) och sektorsspecifika myndigheter, som Post- och telestyrelsen (PTS), att hantera dessa rapporter.**

- **Tillsyn och sanktioner**
  För att säkerställa efterlevnad kräver NIS2 att medlemsstaterna utser tillsynsmyndigheter med befogenhet att genomföra revisioner och utfärda sanktioner. Sanktionerna är betydligt strängare än i NIS1:
  - **Väsentliga enheter riskerar böter på upp till 10 miljoner euro eller 2 % av den globala årsomsättningen, beroende på vilket belopp som är högst.**
  - **Viktiga enheter kan få böter på upp till 7 miljoner euro eller 1,4 % av årsomsättningen. Dessutom kan ledningen (t.ex. VD och styrelse) hållas personligt ansvarig för att säkerställa att organisationen följer direktivet. I Sverige förväntas MSB leda tillsynen för de flesta sektorer, medan Finansinspektionen och Energimyndigheten hanterar finans respektive energi.**
- **Internationellt samarbete**
  NIS2 betonar samverkan mellan medlemsstater och internationella partners. Viktiga mekanismer inkluderar:
  - **European Cyber Crises Liaison Organisation Network (EU-CyCLONe): Ett nätverk för att koordinera responsen på storskaliga cyberkriser, som en attack mot flera länders elnät.**
  - **CSIRT-nätverket: Förstärkt samarbete mellan nationella incidentrespons-team för att dela underrättelser och bästa praxis.**
  - **Informationsdelning: Plattformar för att utbyta data om hot mellan offentlig och privat sektor, samt med icke-EU-länder som NATO-allierade. För Sverige, som Natomedlem, är detta samarbete avgörande för att hantera hot från aktörer som Ryssland, särskilt i Östersjöregionen.**

Jämförelse med NIS1: Vad är nytt?

För att förstå NIS2:s betydelse är det viktigt att jämföra det med NIS1. Här är de huvudsakliga skillnaderna:

- **Bredare tillämpningsområde: NIS1 fokuserade på ett begränsat antal sektorer (energi, transport, finans, hälso- och sjukvård, vatten och digitala tjänster). NIS2 utökar detta till att inkludera livsmedel, avfallshantering, kemi, rymdteknik och offentlig förvaltning, vilket återspeglar en mer holistisk syn på samhällsviktiga tjänster.**
- **Strängare krav: NIS1 hade vaga riktlinjer för säkerhetsåtgärder, vilket ledde till inkonsekvent implementering. NIS2 specificerar konkreta åtgärder, som leverantörskedjesäkerhet och utbildning, och harmoniserar standarder över EU.**
- **Snabbare rapportering: NIS1 krävde rapportering "utan onödigt dröjsmål", vilket ofta var otydligt. NIS2:s 24-timmarsregel tvingar fram snabbare respons.**
- **Hårdare sanktioner: NIS1:s sanktioner var ofta symboliska, medan NIS2:s böter är utformade för att vara avskräckande, särskilt för stora företag.**
- **Ledningsansvar: NIS2:s krav på att hålla ledningen personligt ansvarig är en nyhet, vilket sätter press på beslutsfattare att prioritera cybersäkerhet.**
- **Stärkt samarbete: NIS1 hade begränsade mekanismer för gränsöverskridande samordning. NIS2:s EU-CyCLONe och CSIRT-nätverk är mer robusta och anpassade till dagens hot.**

Dessa förändringar gör NIS2 till ett mer kraftfullt verktyg, men också mer krävande för medlemsstater och organisationer. För Sverige innebär det en möjlighet att stärka cybersäkerheten, men också en utmaning att mobilisera resurser och samordning.

Sektorer i fokus: Hur NIS2 påverkar Sverige

För att göra NIS2:s implikationer konkreta, låt oss titta på tre sektorer som är centrala i Sverige och hur direktivet påverkar dem:

- **Energi**

  Energisektorn är ryggraden i ett modernt samhälle, och Sverige, med sin blandning av vattenkraft, kärnkraft och förnybar energi, är inget undantag. En cyberattack mot ett företag som Vattenfall kunde störa elförsörjningen till miljontals hushåll, med konsekvenser för allt från sjukvård till industri. NIS2 klassar energibolag som väsentliga enheter och kräver att de genomför regelbundna riskanalyser, säkrar sina SCADA-system (som styr elnätet) och rapporterar incidenter snabbt. Ett exempel är en hypotetisk attack där hackare

manipulerar ett elnäts styrsystem för att orsaka strömavbrott. NIS2:s krav på leverantörskedjesäkerhet innebär också att Vattenfall måste granska sina underleverantörer, som ofta tillhandahåller programvara eller hårdvara från globala aktörer.

- **Hälso- och sjukvård**
  Svenska sjukhus, som Region Stockholm eller Sahlgrenska, är beroende av digitala system för patientjournaler, operationsplanering och medicinsk utrustning. En ransomware-attack mot ett sjukhus 2023 visade hur snabbt vård kan lamslås när system låses. NIS2 kräver att hälso- och sjukvårdsaktörer implementerar kryptering, utbildar personal i cybersäkerhet och etablerar rutiner för incidenthantering. Detta är särskilt viktigt eftersom attacker mot vårdsektorn ofta utnyttjar mänskliga misstag, som att en anställd klickar på en skadlig länk. Direktivet tvingar också regioner att granska tredjepartsleverantörer, som företag som tillhandahåller molnbaserade journalsystem.
- **Digital infrastruktur**
  Sverige är hem för globala techföretag som Ericsson och datacenter som används av molnleverantörer som Amazon Web Services och Microsoft Azure. Dessa aktörer klassas som väsentliga eller viktiga enheter under NIS2, beroende på deras storlek och roll. En attack mot ett datacenter kunde störa tjänster för miljontals användare, från banker till streamingplattformar. NIS2:s krav på tekniska skyddsåtgärder, som brandväggar och intrångsdetektering, samt snabb incidentrapportering, är utformade för att minimera sådana risker. Direktivet betonar också vikten av att säkra 5G-nätverk, en prioritet för Sverige efter debatten om kinesiska leverantörer som Huawei.

Dessa exempel visar att NIS2 inte är en abstrakt regel – det är ett ramverk som direkt påverkar hur Sverige fungerar som samhälle.

NIS2 i EU:s cybersäkerhetsstrategi

NIS2 är inte en isolerad reform utan en del av EU:s bredare strategi för att bli en global ledare inom cybersäkerhet. Strategin, som lanserades 2020 och uppdaterades 2023, vilar på tre pelare: motståndskraft, teknologisk suveränitet och internationellt ledarskap. NIS2 bidrar till dessa mål på flera sätt:

- **Motståndskraft: Genom att harmonisera säkerhetskrav och stärka incidenthantering gör NIS2 EU:s medlemsstater mer motståndskraftiga mot**

attacker. Detta är särskilt viktigt i ljuset av händelser som Rysslands cyberattacker mot Ukraina, som också spillt över till EU.

- **Teknologisk suveränitet: NIS2:s fokus på leverantörskedjesäkerhet syftar till att minska beroendet av icke-europeiska aktörer, som kinesiska teknikföretag, och främja inhemsk innovation.**
- **Internationellt ledarskap: Genom att etablera höga standarder för cybersäkerhet positionerar EU sig som en förebild för andra regioner. NIS2:s samarbetsmekanismer, som EU-CyCLONe, möjliggör också partnerskap med aktörer som NATO och USA.**

För Sverige, som både EU-medlem och Natomedlem, är denna strategi en möjlighet att stärka sin roll i det globala cybersäkerhetsekosystemet. Men det kräver också att Sverige balanserar EU:s krav med nationella prioriteringar, som skyddet av Östersjöregionens infrastruktur.

Utmaningar och möjligheter

NIS2-direktivet är ambitiöst, men det är inte utan utmaningar. De strikta kraven på rapportering och säkerhetsåtgärder kan vara betungande för mindre organisationer, särskilt kommuner och småföretag, som ofta saknar resurser och expertis. Implementeringstiden – nationell lagstiftning ska vara på plats senast oktober 2024, med full effekt 2025/2026 – är också snäv, vilket sätter press på både myndigheter och näringsliv. Dessutom väcker ledningsansvaret och sanktionerna frågor om rättvisa och praktisk tillämpning. Kan en kommunal chef realistiskt hållas ansvarig för en attack som utnyttjar globala sårbarheter?

Ändå erbjuder NIS2 betydande möjligheter. Genom att tvinga fram enhetliga standarder kan det minska fragmenteringen i EU:s cybersäkerhet och skapa en starkare försvarslinje mot hot. För Sverige kan direktivet stimulera investeringar i utbildning och forskning, stärka näringslivets konkurrenskraft och förbättra samarbetet med internationella partners. Om Sverige kan navigera implementeringsutmaningarna, har NIS2 potential att inte bara skydda samhället utan också positionera landet som en ledare inom cybersäkerhet.

Mot en ny standard

NIS2-direktivet är mer än en samling regler – det är en vision för ett säkrare digitalt Europa. Genom att utöka skyddet för samhällsviktiga tjänster, införa strikta säkerhetskrav och främja samarbete lägger det grunden för en värld där cyberhot inte längre kan diktera villkoren. För Sverige är detta en möjlighet att bygga en motståndskraft som matchar landets teknologiska ambitioner.

I nästa kapitel vänder vi blicken mot Sverige och undersöker hur NIS2 implementeras i praktiken. Vi utforskar lagstiftningsprocessen, kommunernas utmaningar och

näringslivets anpassning – och frågar oss hur Sverige kan förvandla direktivets krav till en nationell styrka.

Kapitel 3: Sverige och NIS2: Implementeringens utmaningar

En nationell kraftsamling

När NIS2-direktivet trädde i kraft i januari 2023 markerade det början på en ny era för cybersäkerhet i Europa. För Sverige, ett land där digitala system genomsyrar allt från sjukvård till elförsörjning, är direktivet inte bara en EU-förordning – det är en nationell prioritet. Men att omvandla NIS2:s ambitiösa krav till praktisk verklighet är ingen enkel uppgift. Det kräver lagstiftning, resurser, samordning och, kanske viktigast, en kulturförändring där cybersäkerhet blir en självklar del av vardagen för kommuner, företag och myndigheter.

Sverige står inför en dubbel utmaning: att uppfylla NIS2:s strikta tidsramar – nationell lagstiftning ska vara på plats senast oktober 2024, med full implementering 2025/2026 – och att göra det i en tid av ekonomiska och geopolitiska spänningar. Kommuner kämpar med begränsade budgetar, småföretag saknar teknisk expertis, och bristen på cybersäkerhetsspecialister är akut. Samtidigt är trycket från hot som ransomware, statligt sponsrat spionage och sabotage mot kritisk infrastruktur större än någonsin.

Detta kapitel tar oss in i hjärtat av Sveriges implementering av NIS2. Vi utforskar lagstiftningsprocessen, de myndigheter som leder arbetet, och de hinder som kommuner och näringsliv står inför. Genom en fallstudie av en fiktiv kommun belyser vi de praktiska utmaningar som definierar denna resa. Slutligen reflekterar vi över hur Sverige kan övervinna dessa hinder för att inte bara uppfylla NIS2:s krav, utan också stärka sin position som en ledare inom cybersäkerhet.

Lagstiftningsprocessen: Från direktiv till svensk lag

Att införliva NIS2 i svensk lagstiftning är en komplex process som kräver samordning mellan regering, riksdag, myndigheter och intressenter från näringslivet. Direktivet måste vara implementerat i nationell lag senast den 17 oktober 2024, och Sverige har tagit flera steg för att möta denna deadline.

- **Utredningen (SOU 2024:47): I början av 2024 presenterades en statlig utredning, *Cybersäkerhet i samhällsviktiga tjänster* (SOU 2024:47), som kartlade hur NIS2 ska integreras i svensk lag. Utredningen föreslår ändringar i säkerhetsskyddslagen (2018:585) för att täcka NIS2:s krav på säkerhetsåtgärder och incidentrapportering. Den rekommenderar också en ny**

lag specifikt för NIS2, som ska reglera tillsyn, sanktioner och rapporteringskrav för väsentliga och viktiga enheter. Ett särskilt fokus ligger på att anpassa reglerna till Sveriges decentraliserade struktur, där kommuner och regioner spelar en stor roll i samhällsviktiga tjänster.

- **Tidsplan: Ett lagförslag baserat på utredningen förväntas läggas fram våren 2025, med målet att träda i kraft senast oktober 2025. Detta ger organisationer tid att förbereda sig inför full implementering 2026. Men tidsramen är snäv, särskilt för kommuner och småföretag som redan kämpar med att uppgradera sina system.**
- **Ansvariga myndigheter: Myndigheten för samhällsskydd och beredskap (MSB) är den primära samordnaren för NIS2-implementeringen och förväntas fungera som tillsynsmyndighet för de flesta sektorer. Andra myndigheter, som Post- och telestyrelsen (PTS) för telekom, Finansinspektionen för finanssektorn och Energimyndigheten för energi, kommer att ha sektorsspecifika tillsynsuppdrag. Nationellt cybersäkerhetscenter (NCSC), som samlar expertis från Försvarsmakten, Säkerhetspolisen, FRA och MSB, spelar en nyckelroll i att ge tekniskt stöd och koordinera incidenthantering.**
- **Samråd med näringslivet: Regeringen har engagerat branschorganisationer som Svenskt Näringsliv och Teknikföretagen för att säkerställa att näringslivets perspektiv beaktas. Detta är särskilt viktigt för små och medelstora företag, som ofta saknar resurser att navigera komplexa regelverk.**

Trots dessa ansträngningar är lagstiftningsprocessen inte utan risker. Sverige har en tradition av noggranna utredningar, vilket kan leda till förseningar. Dessutom måste lagarna balansera NIS2:s krav med andra regelverk, som dataskyddsförordningen (GDPR), vilket skapar juridiska och praktiska utmaningar.

Resurser och finansiering: En droppe i havet?

Att implementera NIS2 kräver betydande resurser – både ekonomiska och mänskliga. Regeringen har avsatt 196 miljoner kronor i budgeten för 2025 för cybersäkerhet, varav en del är öronmärkt för NIS2-relaterade åtgärder:

- **100 miljoner kronor till NCSC för att stärka dess kapacitet för hotanalys och incidenthantering.**
- **50 miljoner kronor till kampanjen “Tänk säkert”, som syftar till att öka medvetenheten om cybersäkerhet bland allmänheten och småföretag.**
- **46 miljoner kronor till MSB och andra myndigheter för att utveckla riktlinjer, utbildningsprogram och stöd till kommuner.**

Ytterligare finansiering planeras fram till 2029, särskilt för att hjälpa kommuner och regioner att uppfylla NIS2:s krav. Men dessa summor är blygsamma i förhållande till behoven. En rapport från MSB 2024 uppskattar att Sveriges kommuner behöver investera minst 2 miljarder kronor fram till 2030 för att nå en grundläggande nivå av cybersäkerhet, inklusive uppgraderingar av IT-system, utbildning och rekrytering av personal.

Bristen på kvalificerade cybersäkerhetsexperter är en ännu större flaskhals. Sverige producerar färre än 500 specialister per år, medan behovet uppskattas till tusentals. Konkurrensen om talang är hård, och offentliga aktörer som kommuner kan sällan matcha lönerna i privata sektorn. Regeringen har lanserat initiativ för att öka antalet utbildningsplatser, men effekterna kommer inte att märkas förrän om flera år.

Kommunerna i frontlinjen: En fallstudie

För att förstå de praktiska utmaningarna med NIS2, låt oss titta på en fiktiv men realistisk kommun, Västhamn, med 50 000 invånare. Västhamn är typisk för många svenska kommuner: den driver skolor, äldreomsorg och VA-tjänster, men dess IT-avdelning består av fem personer, varav endast en har grundläggande kunskaper i cybersäkerhet. Budgeten är ansträngd, och de flesta resurser går till välfärdstjänster. År 2023 drabbades Västhamn av en ransomware-attack som låste deras system för löneutbetalningar och skoladministration. Attacken, som utnyttjade en ouppdaterad server, kostade kommunen 3 miljoner kronor i återställningskostnader och konsulter. Personalen hade ingen utbildning i att identifiera phishing-mejl, och det saknades rutiner för incidenthantering. När NIS2 träder i kraft klassas Västhamn som en väsentlig enhet på grund av dess roll i samhällsviktiga tjänster, vilket innebär att den måste:

- **Genomföra regelbundna riskanalyser av sina IT-system.**
- **Implementera tekniska skyddsåtgärder, som kryptering och multifaktorautentisering.**
- **Rapportera incidenter till MSB inom 24 timmar.**
- **Utbilda all personal i cybersäkerhet.**
- **Granska säkerheten hos leverantörer, som det företag som tillhandahåller kommunens molnbaserade skolplattform.**

För Västhamn är detta en monumental uppgift. Kommunens IT-budget är 10 miljoner kronor per år, och en uppskattning visar att NIS2-kraven skulle kräva ytterligare 5 miljoner kronor årligen – pengar som inte finns. Personalen är redan överbelastad, och att rekrytera en kvalificerad cybersäkerhetsexpert är omöjligt med de löner kommunen kan erbjuda. Dessutom är samordningen med MSB och andra kommuner svag, vilket gör att Västhamn känner sig ensam i sin kamp.

Västhamns situation är inte unik. En kartläggning från 2024 visar att över 60 % av Sveriges 290 kommuner saknar grundläggande cybersäkerhetsåtgärder, och många har aldrig genomfört en riskanalys. NIS2 tvingar fram en förändring, men utan riktat stöd riskerar kommuner att hamna efter, vilket gör dem till svaga länkar i Sveriges cybersäkerhet.

Näringslivets anpassning: En ojämn resa

Sveriges näringsliv, från globala jättar som Ericsson till små familjeföretag, påverkas också av NIS2. Stora aktörer inom energi, telekom och finans – som Vattenfall, Telia och SEB – är väl rustade för att hantera direktivets krav. De har dedikerade cybersäkerhetsteam, betydande budgetar och erfarenhet av att navigera internationella regelverk. För dessa företag är NIS2 en möjlighet att stärka sitt rykte och konkurrenskraft genom att visa att de uppfyller höga säkerhetsstandarder.

Små och medelstora företag (SMF), som står för 99 % av Sveriges företag, står dock inför större utmaningar. Många SMF klassas som viktiga enheter under NIS2, särskilt om de levererar tjänster till samhällsviktiga sektorer. Ett exempel är ett litet IT-företag som tillhandahåller mjukvara till en kommuns VA-system. Detta företag måste nu genomföra riskanalyser, säkra sin leverantörskedja och rapportera incidenter – krav som kan kosta tiotusentals kronor och kräva expertis de inte har.

En undersökning från Svenskt Näringsliv 2024 visar att 70 % av SMF inte är medvetna om NIS2:s krav, och ännu färre har börjat förbereda sig. Kostnaderna för att uppfylla direktivet – inklusive konsulter, systemuppgraderingar och utbildning – kan vara förlamande för företag med små marginaler. Regeringen och branschorganisationer har lanserat informationskampanjer, men dessa når ofta inte fram till de minsta aktörerna.

Myndigheternas roll: Samordning under press

Sveriges myndigheter är ryggraden i NIS2-implementeringen, men de står inför sina egna utmaningar. MSB, som leder arbetet, har fått ett utökat mandat men kämpar med att bygga upp kapacitet för tillsyn och stöd. Att övervaka hundratals väsentliga och viktiga enheter kräver betydande resurser, och MSB:s personalstyrka är redan ansträngd. Sektorsspecifika myndigheter, som PTS och Finansinspektionen, måste också utveckla expertis för att hantera NIS2:s tekniska krav, vilket kan leda till inkonsekvenser i tillsynen.

NCSC är en ljuspunkt i detta landskap. Genom att samla expertis från flera myndigheter har centret blivit en viktig resurs för att analysera hot och stödja organisationer. Men NCSC:s mandat är primärt rådgivande, och det saknar befogenheter att tvinga fram åtgärder. Ett förslag från SOU 2024:47 är att ge NCSC ett starkare operativt mandat, men detta har väckt debatt om hur mycket makt som bör centraliseras.

Balansen med GDPR och andra regelverk

En oväntad utmaning är hur NIS2 interagerar med andra lagar, särskilt dataskyddsförordningen (GDPR). NIS2:s krav på snabb incidentrapportering – inom 24 timmar – kan innebära att organisationer måste dela känsliga uppgifter, som personuppgifter, med myndigheter innan de fullyllytt GDPR:s krav på dataskydd. Detta skapar en juridisk gråzon som utredningen SOU 2024:47 försöker adressera genom att föreslå tydliga riktlinjer för hur uppgifter ska hanteras. Men utan klarhet riskerar organisationer att hamna i en situation där de bryter mot ett regelverk för att uppfylla ett annat.

Mot en framtid av motståndskraft

Sveriges implementering av NIS2 är en resa kantad av utmaningar, men också möjligheter. Kommuner som Västhamn kan, med rätt stöd, bygga en cybersäkerhet som skyddar invånarna från framtida attacker. Näringslivet kan använda NIS2 som en språngbräda för att stärka sin konkurrenskraft. Och myndigheter kan, genom samordning och innovation, skapa ett ramverk som gör Sverige till en förebild inom cybersäkerhet.

Men framgång kräver handling. Regeringen måste öka finansieringen till kommuner, snabba på rekryteringen av specialister och stärka samordningen mellan aktörer. Utan dessa åtgärder riskerar NIS2 att bli en pappersprodukt – ambitiös i teorin, men ineffektiv i praktiken. I nästa kapitel vänder vi blicken mot en av NIS2:s mest kritiska aspekter: säkerheten i leverantörskedjor. Vi utforskar hur Sverige kan skydda sina globala beroenden och vad detta betyder för nationell suveränitet.

Kapitel 4: Leverantörskedjor och globala beroenden

Den osynliga ryggraden

I november 2024 kastades Sverige in i en geopolitisk storm när två undervattenskablar i Östersjön – avgörande för internettrafiken mellan Sverige, Finland och Baltikum – skadades under misstänkta omständigheter. Spekulationerna om sabotage, med fingrar pekande mot Ryssland, underströk en obehaglig sanning: Sveriges digitala infrastruktur är inte bara beroende av nationella system, utan av en komplex, global leverantörskedja som sträcker sig över kontinenter. Från kinesiska komponenter i 5G-nätverk till amerikanska molntjänster som driver svenska banker – dessa kedjor är både en styrka och en akilleshäl.

NIS2-direktivet (Directive (EU) 2022/2555) erkänner denna verklighet genom att införa strikta krav på säkerhet i leverantörskedjor för organisationer som klassas som väsentliga eller viktiga enheter. För Sverige, ett land djupt integrerat i den globala ekonomin, är detta ett av direktivets mest utmanande men också mest avgörande inslag. Att säkra leverantörskedjor handlar inte bara om teknik – det är en fråga om nationell suveränitet, ekonomisk konkurrenskraft och motståndskraft mot hot som spionage, sabotage och ekonomisk utpressning.

Detta kapitel dyker in i världen av leverantörskedjor och globala beroenden. Vi utforskar vad NIS2:s krav innebär i praktiken, analyserar Sveriges sårbarheter och undersöker fallstudier som Huawei-debatten och kabelbrotten 2024. Slutligen reflekterar vi över hur Sverige kan balansera global integration med nationell säkerhet – och vad detta betyder för framtiden.

Leverantörskedjesäkerhet i NIS2: Vad innebär det?

NIS2-direktivet markerar ett paradigmskifte genom att explicit inkludera leverantörskedjesäkerhet som en central komponent i cybersäkerhet. Tidigare fokuserade cybersäkerhetsregelverk, som NIS1, primärt på organisationers interna system. Men i en värld där en enda kompromitterad komponent – en mikrochip, en mjukvara eller en tredjepartsleverantör – kan orsaka kaos, är detta tillvägagångssätt otillräckligt.

Under NIS2 måste väsentliga och viktiga enheter, såsom energibolag, sjukhus och kommuner, säkerställa att deras leverantörskedjor uppfyller strikta säkerhetsstandarder. Detta innebär:

- **Riskbedömningar: Organisationer måste kartlägga och analysera risker i hela leverantörskedjan, från hårdvarutillverkare till molntjänsteleverantörer.**

- **Kontraktskrav: Leverantörer måste binda sig till säkerhetsåtgärder, som kryptering, regelbundna säkerhetsuppdateringar och incidentrapportering.**
- **Revisioner: Organisationer förväntas genomföra regelbundna granskningar av leverantörers säkerhetsrutiner, inklusive tredjepartsleverantörer som underleverantörer.**
- **Diversifiering: För att minska riskerna uppmuntras organisationer att undvika beroende av enstaka leverantörer, särskilt från högriskländer.**
- **Incidenthantering: Leverantörer måste ha planer för att snabbt rapportera och hantera cyberincidenter som kan påverka kunden.**

Dessa krav är ambitiösa men nödvändiga. En rapport från Försvarets radioanstalt (FRA) 2024 visar att över 40 % av cyberincidenter i Sverige kan spåras till sårbarheter i leverantörskedjan, såsom ouppdaterad mjukvara eller komprometterade tredjepartsleverantörer. NIS2:s fokus på detta område är ett försök att stänga dessa luckor.

Sveriges globala beroenden: En sårbar styrka

Sverige är en öppen, exportdriven ekonomi med en teknologisektor i världsklass. Företag som Ericsson, Volvo och ABB är globala ledare, och landet är hem för datacenter som används av techjättar som Amazon och Microsoft. Men denna integration i den globala ekonomin gör Sverige extremt beroende av internationella leverantörskedjor, särskilt inom teknik. Här är några nyckelområden:

- **Molntjänster: Många svenska organisationer, från banker till kommuner, använder molntjänster från amerikanska leverantörer som Amazon Web Services (AWS), Microsoft Azure och Google Cloud. Dessa tjänster är effektiva men skapar risker för dataläckage och avbrott om leverantören komprometteras.**
- **5G och telekom: Sveriges 5G-nätverk byggs av företag som Nokia och Ericsson, men komponenter kommer ofta från globala underleverantörer. Debatten om kinesiska Huawei har belyst riskerna med att använda leverantörer från länder med potentiella säkerhetshot.**
- **Hårdvara: Mikrochips och andra komponenter i allt från medicinsk utrustning till elnät tillverkas ofta i Asien, särskilt i Kina och Taiwan. En störning i dessa kedjor – som under pandemin 2020–2021 – kan lamslå kritiska system.**
- **Mjukvara: Svenska organisationer är beroende av mjukvara från globala aktörer, som Microsoft för operativsystem eller Oracle för databaser.**

Sårbarheter i dessa produkter, som Log4j-sårbarheten 2021, kan utnyttjas i stor skala.

Sveriges beroende av globala leverantörer förstärks av dess begränsade inhemska kapacitet. Till skillnad från större ekonomier som USA eller Kina har Sverige inte resurserna att producera alla kritiska komponenter själv. Detta gör NIS2:s krav på leverantörskedjesäkerhet både avgörande och svåra att uppfylla.

Fallstudie 1: Huawei och 5G-debatten

Ett av de mest omtalade exemplen på leverantörskedjerisker är Sveriges beslut 2020 att utesluta kinesiska Huawei från sitt 5G-nätverk. Beslutet, fattat av Post- och telestyrelsen (PTS) på rekommendation av Säkerhetspolisen och Försvarsmakten, motiverades av nationella säkerhetsrisker. Huawei, som kontrolleras av den kinesiska regeringen, ansågs kunna användas för spionage eller sabotage, särskilt genom bakdörrar i deras utrustning.

Reaktionerna var blandade. Operatörer som Telia och Tele2, som redan använde Huawei-utrustning, tvingades byta till dyrare alternativ från Nokia och Ericsson, vilket ökade kostnaderna för 5G-utbyggnaden. Kina hotade med ekonomiska repressalier, och vissa kritiker menade att beslutet var politiskt snarare än tekniskt motiverat. Men för Sverige var det ett tydligt ställningstagande: leverantörskedjesäkerhet är en fråga om suveränitet.

NIS2 förstärker denna approach. Direktivet uppmuntrar medlemsstater att identifiera och mitigera risker från högriskleverantörer, särskilt i kritiska sektorer som telekom. För Sverige innebär detta att operatörer måste granska inte bara primära leverantörer som Nokia, utan också deras underleverantörer, som kan använda komponenter från osäkra källor. Detta är en resurskrävande process, men en nödvändig sådan i en tid då geopolitiska spänningar gör teknologiska beroenden till ett vapen.

Fallstudie 2: Kabelbrotten 2024

Händelserna i Östersjön hösten 2024 – där två undervattenskablar skadades under misstänkta omständigheter – kastade ljus på en annan aspekt av leverantörskedjesäkerhet: fysisk infrastruktur. Dessa kablar, som ägs och underhålls av internationella konsortier, är livsviktiga för Sveriges internetanslutning. Men deras ägarstruktur och underhåll är ofta ogenomskinliga, vilket gör dem sårbara för sabotage.

NIS2 adresserar detta genom att kräva att operatörer av digital infrastruktur, som kabelägare och datacenter, implementerar säkerhetsåtgärder för både fysiska och digitala tillgångar. I Sverige har detta lett till diskussioner om att stärka skyddet av undervattensinfrastruktur, inklusive krav på att operatörer kartlägger sina leverantörskedjor och identifierar risker. Men utmaningen är stor: många kablar passerar internationella vatten, och ägarna är ofta baserade utanför EU, vilket gör det svårt att genomföra revisioner eller verkställa sanktioner.

Utmaningar med leverantörskedjesäkerhet

Att uppfylla NIS2:s krav på leverantörskedjesäkerhet är ingen enkel uppgift för Sverige. Här är de största hindren:

- **Global komplexitet: Leverantörskedjor är ofta djupt sammanflätade, med dussintals aktörer spridda över världen. Att kartlägga och säkra varje länk är tidskrävande och dyrt, särskilt för små organisationer som kommuner.**
- **Resursbrist: Revisioner och riskanalyser kräver expertis som många svenska organisationer saknar. Småföretag och kommuner har ofta inte råd att anlita konsulter eller genomföra omfattande granskningar.**
- **Geopolitiska spänningar: Beslut som att utesluta kinesiska leverantörer kan leda till handelskonflikter, vilket sätter press på Sveriges exportberoende ekonomi.**
- **Begränsad nationell kapacitet: Sverige saknar förmågan att producera många kritiska komponenter, som mikrochips, vilket gör det svårt att minska beroendet av utländska aktörer.**
- **Juridiska gråzoner: Att kräva att utländska leverantörer följer NIS2:s standarder är svårt, särskilt om de är baserade utanför EU. Detta skapar en risk för att säkerhetskraven bara delvis implementeras.**

Möjligheter för Sverige

Trots utmaningarna erbjuder NIS2:s fokus på leverantörskedjesäkerhet flera möjligheter:

- **Stärkt motståndskraft: Genom att säkra leverantörskedjor kan Sverige minska risken för attacker som utnyttjar tredjepartsleverantörer, vilket stärker hela samhällets cybersäkerhet.**
- **Ekonomisk konkurrenskraft: Företag som uppfyller NIS2:s krav kan positionera sig som pålitliga partners på den globala marknaden, särskilt inom tech och infrastruktur.**
- **Innovation: Kraven på leverantörskedjesäkerhet kan stimulera utvecklingen av inhemska lösningar, som säkra mjukvaruplattformar eller lokala datacenter.**
- **Internationellt samarbete: Som Natomedlem och EU-land kan Sverige dra nytta av samarbeten, som EU:s CSIRT-nätverk, för att dela information om risker i leverantörskedjor.**

Mot nationell suveränitet

Leverantörskedjesäkerhet är inte bara en teknisk fråga – det är en strategisk prioritet som berör Sveriges suveränitet. I en värld där teknologi är ett slagfält måste Sverige minska sitt beroende av osäkra leverantörer utan att isolera sig från den globala ekonomin. Detta kräver en balansgång: att samarbeta med betrodda partners, investera i nationell kapacitet och bygga en kultur där säkerhet är en del av varje affärsbeslut.

NIS2:s krav är ett första steg, men de räcker inte ensamma. Sverige behöver en nationell strategi för leverantörskedjesäkerhet, med finansiering för forskning, stöd till småföretag och tydliga riktlinjer för hur organisationer kan navigera globala beroenden. I nästa kapitel utforskar vi hur Sverige kan stärka sitt internationella samarbete – från EU:s EU-CyCLONe till Natos cyberförsvar – för att möta hot som inte respekterar gränser.

Kapitel 5: Samordning och samarbete: Nationellt och internationellt

Tillsammans mot hoten

I februari 2025 samlades representanter från Försvarsmakten, Säkerhetspolisen, Myndigheten för samhällsskydd och beredskap (MSB), och flera privata företag vid Nationellt cybersäkerhetscenter (NCSC) i Stockholm. Målet var en simulerad cyberattack mot Sveriges elnät, där en fiktiv statlig aktör försökte sabotera kritisk infrastruktur. Övningen, inspirerad av verkliga händelser som kabelbrotten i Östersjön 2024, visade styrkan i samverkan: genom att dela information i realtid kunde aktörerna identifiera angriparens metoder och begränsa skadan. Men övningen avslöjade också svagheter – kommuner saknade resurser att delta fullt ut, och vissa privata aktörer tvekade att dela känslig data av konkurrensskäl.

Denna scen understryker en central sanning i cybersäkerhetens värld: inga aktörer, oavsett hur välutrustade, kan möta dagens hot ensamma. NIS2-direktivet (Directive (EU) 2022/2555) erkänner detta genom att betona samordning och samarbete som hörnstenar i Europas cybersäkerhetsstrategi. För Sverige, ett land med en decentraliserad struktur och en nyckelroll i både EU och NATO, är detta särskilt relevant. Från nationella myndigheter till lokala kommuner, från privata företag till internationella allierade – cybersäkerhet kräver en gemensam front.

Detta kapitel utforskar hur Sverige bygger denna front. Vi analyserar NCSC:s roll som nav för nationell samordning, undersöker offentlig-privata partnerskap, och granskar Sveriges bidrag till internationellt samarbete genom EU:s och NATO:s mekanismer. Genom exempel på framgångar och utmaningar visar vi varför samarbete är både en

möjlighet och en nödvändighet – och hur Sverige kan stärka sin position i en värld där cyberhot inte respekterar gränser.

Nationellt cybersäkerhetscenter (NCSC): Sveriges samordningsnav

Etablerat 2021, är NCSC hjärtat i Sveriges nationella cybersäkerhetsarbete. Centret, som drivs gemensamt av MSB, Försvarsmakten, Säkerhetspolisen och Försvarets radioanstalt (FRA), fungerar som en plattform för att samla expertis, analysera hot och stödja organisationer i att hantera cyberincidenter. Under NIS2 har NCSC:s roll förstärkts, särskilt i samband med direktivets krav på incidentrapportering och informationsdelning.

- **Uppgifter: NCSC ansvarar för att ta emot och analysera incidentrapporter från väsentliga och viktiga enheter, enligt NIS2:s 24-timmarsregel. Centret genomför också hotjakt, där det proaktivt söker efter sårbarheter i kritiska system, och erbjuder tekniskt stöd till kommuner och företag. Under 2024 hanterade NCSC över 200 betydande incidenter, från ransomware mot kommuner till försök till spionage mot försvarsindustrin.**
- **Resurser: Budgeten för 2025 avsätter 100 miljoner kronor till NCSC, en ökning från föregående år, för att stärka dess analyskapacitet och utöka personalen. Men med endast cirka 50 anställda är centret underdimensionerat i förhållande till behoven.**
- **Utmaningar: NCSC:s mandat är primärt rådgivande, vilket begränsar dess förmåga att tvinga fram åtgärder. Ett förslag från utredningen SOU 2024:47 är att ge centret ett starkare operativt mandat, men detta har väckt frågor om balansen mellan centralisering och sektorsspecifik autonomi.**

Trots dessa utmaningar är NCSC en framgångssaga. Ett exempel är dess respons på en DDoS-attack mot flera svenska banker hösten 2024. Genom att koordinera med bankerna, PTS och internationella partners kunde NCSC snabbt identifiera angriparens infrastruktur och mildra attacken. Denna typ av samverkan är precis vad NIS2 syftar till att förstärka.

Offentlig-privat samarbete: En nödvändig allians

Cybersäkerhet i Sverige är inte bara en fråga för staten – privata företag driver mycket av den kritiska infrastrukturen, från elnät till telekom. NIS2 betonar vikten av offentlig-privata partnerskap (PPP) för att dela information, utveckla bästa praxis och stärka motståndskraften. I Sverige har detta samarbete en stark tradition, men det står också inför hinder.

- **Framgångar: Ett exempel är *Säkerhetsforum*, en plattform där företag som Ericsson, Vattenfall och SEB möter myndigheter för att diskutera hot och lösningar. Under 2024 lanserade forumet en gemensam databas för att dela**

anonymiserad information om cyberincidenter, vilket hjälpte småföretag att identifiera nya phishing-trender. Ett annat exempel är samarbetet mellan MSB och techföretag för att utveckla riktlinjer för säkra molntjänster, i linje med NIS2:s krav på leverantörskedjesäkerhet.

- **Utmaningar: Trots framgångarna finns hinder. Många företag tvekar att dela känslig information om incidenter av rädsla för konkurrensnackdelar eller rättsliga konsekvenser. Små och medelstora företag (SMF), som ofta saknar resurser att delta i forum som Säkerhetsforum, riskerar att hamna utanför. Dessutom kan olika prioriteringar – myndigheter fokuserar på säkerhet, företag på lönsamhet – skapa spänningar.**
- **NIS2:s påverkan: Direktivet tvingar fram ökad transparens genom sina rapporteringskrav, vilket kan stärka offentlig-privat samarbete. Men för att detta ska fungera behöver Sverige investera i plattformar som gör informationsdelning enkel och säker, särskilt för SMF.**

Ett konkret fall är samarbetet efter en ransomware-attack mot en svensk livsmedelsproducent 2023. Genom att dela information via NCSC kunde producenten, tillsammans med MSB och ett cybersäkerhetsföretag, återställa systemen på mindre än 48 timmar. Detta visar potentialen i offentlig-privat samarbete – men också behovet av att inkludera mindre aktörer.

EU-samarbete: EU-CyCLONe och CSIRT-nätverket

NIS2:s fokus på internationellt samarbete är särskilt relevant för Sverige, som är djupt integrerat i EU:s cybersäkerhetsekosystem. Direktivet introducerar flera mekanismer för att stärka samverkan mellan medlemsstater:

- **European Cyber Crises Liaison Organisation Network (EU-CyCLONe): Detta nätverk, etablerat 2021 och förstärkt under NIS2, syftar till att koordinera responsen på storskaliga cyberkriser som påverkar flera länder. Till exempel, om en attack mot elnätet sprider sig från Tyskland till Sverige, kan EU-CyCLONe mobilisera resurser och dela underrättelser i realtid. Sverige har aktivt deltagit i EU-CyCLONe-övningar, inklusive en 2024 där en simulerad attack mot finanssektorn testades.**
- **CSIRT-nätverket: NIS2 stärker samarbetet mellan nationella Computer Security Incident Response Teams (CSIRT). Sveriges CSIRT, drivet av MSB, fungerar som en länk till detta nätverk, vilket möjliggör snabb delning av information om nya hot, som nolldagsexploateringar. Under 2024 bidrog Sveriges CSIRT**

med data om en ny ransomware-variant, vilket hjälpte andra länder att förebygga attacker.

- **Informationsdelning: NIS2 uppmuntrar etableringen av plattformar för att dela hotdata mellan medlemsstater och privata aktörer. EU:s Cybersecurity Competence Centre i Bukarest är en sådan hub, där Sverige bidrar med expertis inom 5G-säkerhet och AI.**

Dessa mekanismer är avgörande för att hantera gränsöverskridande hot, som de DDoS-attacker som drabbade Norden och Baltikum 2024. Men utmaningar kvarstår. Medlemsstater har olika nivåer av cybersäkerhetsmognad, vilket kan leda till ojämn informationsdelning. Dessutom kräver EU-CyCLONe resurser som mindre länder, inklusive Sverige, kan ha svårt att avsätta.

NATO:s roll: Sverige som en cyberallierad

Sveriges inträde i NATO i mars 2024 har förändrat landets roll i det globala cybersäkerhetslandskapet. Som medlem förväntas Sverige bidra till alliansens kollektiva cyberförsvar, och NIS2 kompletterar detta genom att säkerställa att nationella system uppfyller höga säkerhetsstandarder.

- **NATO:s cyberförsvar: Alliansen har utvecklat en robust cybersäkerhetsstrategi, med fokus på avskräckning och snabb respons. Sverige deltar i NATO:s Cyber Coalition, en årlig övning där medlemsländer testar sin förmåga att hantera attacker. Under 2024 bidrog Sverige med expertis om undervattensinfrastruktur, inspirerat av kabelbrotten.**
- **Samarbete med NIS2: Direktivet stärker Sveriges förmåga att bidra till NATO genom att harmonisera nationella standarder med alliansens krav. Till exempel säkerställer NIS2:s rapporteringskrav att Sverige snabbt kan dela information om attacker med NATO:s Cyber Rapid Reaction Team.**
- **Utmaningar: Som ny medlem måste Sverige investera i att integrera sina system med NATO:s, vilket kräver resurser och teknisk expertis. Dessutom skapar Sveriges dubbla roller – som EU-land och NATO-medlem – en balansgång mellan olika samarbetsramverk.**

Ett exempel på framgång är Sveriges bidrag till en NATO-övning 2024, där FRA:s analys av en rysk cyberkampanj delades med allierade, vilket stärkte försvaret mot liknande attacker. Detta visar hur NIS2 och NATO-samarbete kan förstärka varandra.

Utmaningar i samordning och samarbete

Trots framstegen står Sverige inför flera hinder i att maximera samarbetets potential:

- **Fragmentering: Sveriges decentraliserade struktur, med 290 kommuner och flera sektorsmyndigheter, gör samordning svår. Kommuner saknar ofta resurser att delta i nationella eller internationella initiativ.**
- **Rädsla för informationsdelning: Företag och kommuner tvekar att dela data om incidenter på grund av konkurrens eller rättsliga risker, vilket begränsar effektiviteten i offentlig-privata partnerskap.**
- **Resursbrist: NCSC och andra myndigheter är underbemannade, och budgeten för 2025 räcker inte för att täcka alla behov. Internationella åtaganden, som EU-CyCLONe, kräver ytterligare resurser.**
- **Skillnader i kapacitet: På EU-nivå varierar medlemsstaternas cybersäkerhetsförmåga, vilket kan försvaga samarbetet. Sverige, som är relativt avancerat, riskerar att behöva kompensera för svagare länder.**

Möjligheter för Sverige

NIS2:s fokus på samarbete erbjuder flera möjligheter:

- **Ledarskap: Sverige kan positionera sig som en ledare inom cybersäkerhet genom att bidra med expertis till EU och NATO, särskilt inom 5G och kritisk infrastruktur.**
- **Innovation: Offentlig-privata partnerskap kan driva utvecklingen av nya lösningar, som säkra molntjänster eller AI-baserad hotdetektering.**
- **Motståndskraft: Genom att dela information kan Sverige snabbare identifiera och mildra hot, vilket stärker hela samhällets cybersäkerhet.**
- **Globalt inflytande: Som Natomedlem och EU-land kan Sverige påverka internationella standarder och stärka sitt rykte som en pålitlig partner.**

Mot en gemensam framtid

Samordning och samarbete är inte bara en teknisk nödvändighet – det är en strategisk möjlighet för Sverige att bygga en cybersäkerhet som är större än summan av dess delar. NCSC, offentlig-privata partnerskap, EU-CyCLONe och NATO är byggstenar i denna vision, men deras framgång beror på investeringar, tillit och en vilja att övervinna hinder.

I nästa kapitel vänder vi blicken mot en av de mest komplexa frågorna i NIS2:s värld: balansen mellan säkerhet och frihet. Vi utforskar hur Sverige kan skydda sina medborgare från cyberhot utan att kompromissa med integritet och demokratiska värderingar – och vad detta betyder för framtiden.

Kapitel 6: Balansen mellan säkerhet och frihet

En delikat balans

Hösten 2024 drabbades en svensk kommun av en ransomware-attack som låste deras system för socialtjänsten. För att uppfylla NIS2-direktivets krav rapporterade kommunen incidenten till Myndigheten för samhällsskydd och beredskap (MSB) inom 24 timmar, inklusive detaljer om komprometterade personuppgifter. Men när rapporten delades med andra myndigheter och internationella partners, enligt direktivets samarbetskrav, uppstod en oväntad komplikation: dataskyddsombudet hävdade att delningen kunde bryta mot dataskyddsförordningen (GDPR), eftersom berörda medborgare inte informerats i tid. Kommunen hamnade i en omöjlig situation – fångad mellan att skydda samhället och respektera invånarnas rättigheter.

Denna händelse belyser en av de mest komplexa frågorna i NIS2:s värld: hur balanserar vi behovet av robust cybersäkerhet med de demokratiska värderingar som definierar Sverige? NIS2-direktivet, med sina krav på snabb rapportering, ökad övervakning och ledningsansvar, är en kraftfull mekanism för att skydda samhällsviktiga tjänster. Men det väcker också etiska och juridiska dilemman – om integritet, transparens och risken för övervakningssamhälle. Hur säkerställer vi att skyddet mot cyberhot inte urholkar de friheter vi försöker försvara?

Detta kapitel granskar dessa spänningar. Vi utforskar konflikter mellan NIS2 och GDPR, analyserar de etiska implikationerna av AI och övervakning, och reflekterar över ledningsansvarets rättvisa. Slutligen undersöker vi medborgarnas roll i cybersäkerhet och hur Sverige kan bygga en säkerhetskultur som respekterar demokratiska principer. Genom att navigera dessa frågor kan Sverige inte bara implementera NIS2, utan också forma en framtid där säkerhet och frihet går hand i hand.

NIS2 och GDPR: En juridisk konflikt

En av de mest akuta spänningarna i NIS2:s implementering är dess relation till dataskyddsförordningen (GDPR), EU:s ramverk för att skydda personuppgifter. Båda regelverken är hörnstenar i EU:s lagstiftning, men deras mål och metoder kan kollidera:

- **Snabb rapportering vs. dataskydd: NIS2 kräver att organisationer rapporterar betydande cyberincidenter till nationella myndigheter inom 24 timmar, inklusive initiala detaljer om påverkan. Om incidenten involverar personuppgifter – som ett dataintrång i ett sjukhus – kan detta innebära att**

känslig information delas innan organisationen har uppfyllt GDPR:s krav på att informera berörda individer eller genomföra en fullständig konsekvensbedömning. Detta skapar en risk för juridiska sanktioner under GDPR, som kan uppgå till 20 miljoner euro eller 4 % av årsomsättningen.

- **Internationell delning: NIS2:s krav på informationsdelning genom mekanismer som EU-CyCLONe eller CSIRT-nätverket kan innebära att data överförs till andra länder, inklusive utanför EU (t.ex. till NATO-allierade). GDPR ställer strikta krav på sådana överföringar, särskilt till länder utan adekvat dataskydd, vilket kan komplicera samarbetet.**
- **Övervakning och loggning: För att uppfylla NIS2:s säkerhetskrav måste organisationer ofta implementera omfattande loggning av nätverkstrafik och användaraktiviteter. Detta kan leda till insamling av personuppgifter i stor skala, vilket riskerar att bryta mot GDPR:s princip om dataminimering.**

Sveriges utredning (SOU 2024:47) försöker lösa dessa konflikter genom att föreslå riktlinjer för hur organisationer kan balansera rapporteringskrav med dataskydd. Till exempel kan initiala rapporter anonymiseras för att minimera risken för GDPR-överträdelser. Men dessa riktlinjer är fortfarande under utveckling, och många organisationer – särskilt kommuner och småföretag – saknar expertis att navigera gråzonen. Resultatet är en osäkerhet som kan hämma effektiv incidenthantering.

Etiska frågor: Övervakning och AI

NIS2:s krav på avancerade säkerhetsåtgärder, som intrångsdetektering och hotjakt, driver organisationer mot att använda teknologier som artificiell intelligens (AI) och maskininlärning. Dessa verktyg kan snabbt identifiera anomalier i nätverkstrafik eller förutsäga attacker, men de väcker också etiska frågor:

- **Övervakning: AI-baserade system kräver ofta omfattande datainsamling, inklusive övervakning av anställdas beteenden (t.ex. e-post eller webbaktiviteter). Detta kan skapa en känsla av övervakningssamhälle, särskilt i offentliga organisationer som kommuner. En undersökning från 2024 visar att 60 % av svenska anställda är oroliga för att cybersäkerhetsåtgärder inkräktar på deras integritet.**
- **Bias och fel: AI-system är inte felfria. Felaktiga positiva resultat – där oskyldiga aktiviteter flaggas som hot – kan leda till orättvisa konsekvenser, som att anställda misstänks för sabotage. Detta är särskilt problematiskt i sektorer som hälso- och sjukvård, där känsliga data hanteras.**

- **Transparens: Många AI-system är "svarta lådor", där beslutsprocessen är oklar. Om en organisation använder AI för att uppfylla NIS2:s krav, hur kan medborgare eller anställda lita på att besluten är rättvisa?**

Sverige, med sin starka tradition av transparens och medborgarrättigheter, står inför en särskild utmaning. Regeringen har lanserat initiativ för att utveckla etiska riktlinjer för AI i cybersäkerhet, men dessa är fortfarande i sin linda. NIS2:s implementering måste åtföljas av tydliga ramverk för att säkerställa att teknologin används ansvarsfullt.

Ledningsansvar: Rättvist eller repressivt?

En av NIS2:s mest kontroversiella aspekter är kravet på att hålla ledningen – som VD:ar och styrelseledamöter – personligt ansvarig för att säkerställa efterlevnad. Om en organisation misslyckas med att implementera säkerhetsåtgärder eller rapportera incidenter kan ledningen få böter eller andra sanktioner. Detta är ett försök att tvinga fram prioritering av cybersäkerhet på högsta nivå, men det väcker frågor om rättvisa:

- **Praktisk genomförbarhet: I små organisationer, som kommuner eller familjeföretag, har ledningen ofta begränsad teknisk expertis. Är det rimligt att hålla en kommunal chef ansvarig för en attack som utnyttjar en global sårbarhet?**
- **Risk för avskräckning: Stränga sanktioner kan avskräcka kvalificerade personer från att ta ledande roller i utsatta sektorer, särskilt i små organisationer med knappa resurser.**
- **Kulturella skillnader: I Sverige, där ledarskap ofta präglas av konsensus och delegering, kan personligt ansvar kännas främmande. Detta kan skapa spänningar mellan ledning och anställda.**

En hypotetisk situation illustrerar dilemmat: Tänk dig en VD för ett medelstort energibolag som investerar i cybersäkerhet men missar en sårbarhet i en tredjepartsleverantör. Om en attack inträffar, kan VD:n hållas ansvarig trots att hen agerat i god tro. Detta riskerar att skapa en kultur av rädsla snarare än proaktivitet. Sverige behöver tydliga riktlinjer för hur ledningsansvar ska tillämpas, med fokus på rimlighet och stöd snarare än bestraffning.

Medborgarnas roll: Från passiva offer till aktiva försvarare

Cybersäkerhet är inte bara en fråga för myndigheter och företag – medborgarna spelar en avgörande roll. Många cyberattacker, som phishing eller social engineering, utnyttjar mänskliga misstag. NIS2 erkänner detta genom att kräva att organisationer utbildar sin personal, men det saknar direkta mekanismer för att

engagera allmänheten. I Sverige, där digital mognad är hög, finns en unik möjlighet att bygga en säkerhetskultur som involverar alla.

- **Kampanjen "Tänk säkert": Lanserad 2024 med 50 miljoner kronor i finansiering, syftar denna kampanj till att öka medborgarnas medvetenhet om cybersäkerhet. Genom annonser, workshops och online-resurser uppmuntras svenskar att använda starka lösenord, aktivera multifaktorautentisering och känna igen phishing-mejl. Men kampanjen har kritiserats för att inte nå utsatta grupper, som äldre eller småföretagare, som ofta är mål för attacker.**
- **Utbildning i skolor: Sverige har börjat integrera cybersäkerhet i skolundervisningen, med fokus på digital literacy från tidig ålder. Detta är ett långsiktigt projekt, men det kan skapa en generation som är bättre rustad att hantera cyberhot.**
- **Medborgarengagemang: För att maximera effekten behöver Sverige plattformar där medborgare kan rapportera misstänkta incidenter, som phishing-försök, till myndigheter. En sådan "crowdsourcing" av hotdata kunde stärka NCSC:s arbete och ge medborgarna en känsla av ägarskap.**

Ett exempel på medborgarens roll är en incident 2024, där en anställd på en kommun identifierade ett phishing-mejl som försökte stjäla inloggningsuppgifter. Tack vare utbildning från "Tänk säkert" rapporterade anställden mejlet, vilket förhindrade en större attack. Detta visar att medborgare kan vara en första försvarslinje – om de ges rätt verktyg.

Bygga en etisk cybersäkerhet

Att balansera säkerhet och frihet är ingen enkel uppgift, men Sverige har en unik möjlighet att visa vägen. Med sin starka tradition av demokrati, transparens och medborgarengagemang kan landet utveckla en cybersäkerhetsmodell som inte bara skyddar utan också respekterar individen. Här är några förslag:

- **Tydliga riktlinjer för GDPR och NIS2: Regeringen bör snarast fastställa hur organisationer kan uppfylla båda regelverken, till exempel genom anonymiserade rapporter eller standardiserade protokoll.**
- **Etiska ramverk för AI: Sverige bör leda utvecklingen av riktlinjer för AI i cybersäkerhet, med fokus på transparens, rättvisa och medborgarförtroende.**
- **Rimligt ledningsansvar: Sanktioner för ledningen bör kopplas till tydliga kriterier, som brist på grundläggande åtgärder, snarare än oundvikliga incidenter.**

- **Medborgarcentrerad säkerhet: Kampanjer som “Tänk säkert” bör skalas upp och anpassas för att nå alla grupper, med fokus på praktiska, användarvänliga råd.**

Mot en framtid i balans

NIS2-direktivet är en möjlighet att bygga en cybersäkerhet som skyddar Sverige utan att offra dess demokratiska värderingar. Men detta kräver mer än tekniska lösningar – det kräver en kultur där säkerhet och frihet ses som ömsesidigt förstärkande. Genom att lösa konflikter med GDPR, använda AI ansvarsfullt, tillämpa ledningsansvar rättvist och engagera medborgarna kan Sverige skapa en modell som inspirerar andra.

I nästa kapitel vänder vi blicken mot framtiden. Vi utforskar hur Sverige kan gå bortom NIS2:s krav för att bli en global ledare inom cybersäkerhet – och vilka hot och möjligheter som väntar i en värld av kvantdatorer, AI och klimatrelaterade risker.

Kapitel 7: Framtiden för Sveriges cybersäkerhet

En vision för motståndskraft

Våren 2025, under en nationell cybersäkerhetskonferens i Stockholm, presenterade en ung forskare från KTH en prototyp för en ny krypteringsmetod som kunde motstå attacker från kvantdatorer. Publiken, bestående av beslutsfattare, techföretag och internationella delegater, applåderade entusiastiskt. Denna innovation, finansierad genom ett samarbete mellan regeringen och näringslivet, var inte bara en teknisk bedrift – det var en signal om Sveriges ambition att leda den globala cybersäkerhetsarenan. Men för att förverkliga denna vision krävs mer än enstaka genombrott. Det kräver en strategisk satsning på att möta morgondagens hot och möjligheter.

NIS2-direktivet (Directive (EU) 2022/2555) har lagt grunden för en robust cybersäkerhet i Sverige, med krav på säkerhetsåtgärder, rapportering och samarbete. Men direktivet är bara ett första steg. I en värld där teknologin utvecklas exponentiellt och hoten blir alltmer sofistikerade, måste Sverige tänka bortom minimikraven. Hur kan landet bygga en cybersäkerhet som inte bara skyddar samhället utan också driver innovation, stärker konkurrenskraften och inspirerar andra nationer?

Detta kapitel blickar framåt mot Sveriges cybersäkerhetsframtid. Vi utforskar de hot som väntar – från kvantdatorer och AI-drivna attacker till klimatrelaterade risker – och erbjuder konkreta rekommendationer för hur Sverige kan bli en global ledare.

Genom att investera i utbildning, forskning och nationell kapacitet kan Sverige forma en framtid där cybersäkerhet är en hörnsten i både säkerhet och välstånd.

Framtida hot: En ny era av komplexitet

Cybersäkerhetshoten 2025 är redan sofistikerade, men de kommande decennierna kommer att introducera nya utmaningar som kräver proaktiv planering. Här är de mest betydande hoten som Sverige måste förbereda sig för:

- **Kvantdatorer: Kvantdatorer, som förväntas bli kommersiellt gångbara inom 10–15 år, kan knäcka dagens krypteringsmetoder, som RSA och AES, på sekunder. Detta hotar allt från banktransaktioner till försvarskommunikation. Redan nu investerar aktörer som Kina och USA miljarder i kvantteknologi, och Sverige riskerar att hamna efter om det inte agerar snabbt.**
- **AI-drivna attacker: Artificiell intelligens används redan för att automatisera phishing, skapa deepfakes och identifiera sårbarheter i system. Framöver kan AI göra attacker ännu mer precisa och svårspårade. En rapport från Säkerhetspolisen 2024 varnar för att statliga aktörer redan experimenterar med AI för hybridkrigföring, som att manipulera opinioner inför val.**
- **Klimatrelaterade cyberrisker: Klimatförändringar skapar nya sårbarheter, som översvämningar som skadar datacenter eller extremväder som stör elnät. Samtidigt kan aktörer utnyttja klimatkriser för att lansera cyberattacker, som att rikta sig mot nödservicesystem under en naturkatastrof. Sverige, med sin ambition att vara klimatneutralt, måste integrera cybersäkerhet i sin klimatanpassning.**
- **Hybridhot och desinformation: Kombinationen av cyberattacker och informationspåverkan kommer att intensifieras, särskilt i geopolitiskt känsliga regioner som Östersjön. Rysslands hybridattacker mot Ukraina visar hur desinformation kan förstärka effekten av tekniska angrepp, och Sverige, som Natomedlem, är ett troligt mål.**
- **IoT och 5G-sårbarheter: Sakernas internet (IoT) och 5G-nätverk gör samhället mer uppkopplat, men också mer sårbart. En komprometterad IoT-enhet, som en smart mätare i ett hem, kan användas för att infiltrera hela nätverk. Sverige, som är ledande inom 5G, måste prioritera säkerheten i dessa teknologier.**

Dessa hot kräver en cybersäkerhetsstrategi som är flexibel, framåtblickande och grundad i innovation. NIS2 lägger en solid bas, men Sverige måste gå längre för att möta framtiden.

Rekommendationer för en ledande cybersäkerhet

För att bli en global ledare inom cybersäkerhet måste Sverige investera i tre nyckelområden: utbildning, forskning och nationell kapacitet. Här är konkreta förslag:

- **Utbildning och kompetensförsörjning**
  Bristen på cybersäkerhetsexperter är en av Sveriges största svagheter. Med färre än 500 kvalificerade specialister producerade per år, och ett behov av tusentals, krävs en kraftsamling:
  - **Nationellt utbildningsprogram: Skapa ett "Cyberakademi"-program i samarbete med universitet, som KTH och Chalmers, för att erbjuda snabbspår till cybersäkerhetsexperter. Programmet bör inkludera stipendier, praktikplatser och fortbildning för offentlig sektor.**
  - **Skolundervisning: Integrera cybersäkerhet i läroplanen från grundskolan, med fokus på digital literacy, kodning och etik. Detta kan bygga en generation som är rustad för framtida hot.**
  - **Offentlig-privat samarbete: Techföretag som Ericsson och Saab kan finansiera utbildningsinitiativ i utbyte mot tillgång till talang, vilket skapar en win-win-situation.**
  - **Mångfald: Satsa på att locka underrepresenterade grupper, som kvinnor och minoriteter, till cybersäkerhetsfältet genom riktade rekryteringskampanjer.**
- **Forskning och innovation**
  Sverige har en stark tradition av teknologisk innovation, men cybersäkerhetsforskning är underfinansierad jämfört med andra länder. För att möta hot som kvantdatorer och AI krävs:
  - **Nationellt forskningscentrum: Etablera ett centrum för cybersäkerhetsforskning, finansierat av regeringen och näringslivet, med fokus på kvantkryptering, AI-säkerhet och IoT. Centret kan samarbeta med NCSC och internationella partners som EU:s Cybersecurity Competence Centre.**
  - **Investeringar: Öka finansieringen för cybersäkerhetsforskning till minst 1 miljard kronor årligen fram till 2030, med fokus på både grundforskning och tillämpade lösningar.**
  - **Startups och innovation: Skapa ett statligt finansierat inkubatorprogram för cybersäkerhetsstartups, som kan utveckla lösningar för 5G, molntjänster och kritisk infrastruktur.**

    - **Internationellt samarbete: Delta i EU:s och NATO:s forskningsprogram för att dra nytta av global expertis och positionera Sverige som en ledare.**
- **Nationell kapacitet och suveränitet**
  Sveriges beroende av globala leverantörskedjor, som diskuterades i Kapitel 4, är en sårbarhet. För att stärka suveräniteten behöver landet:
    - **Inhemsk produktion: Investera i nationell kapacitet för kritiska komponenter, som mikrochips och säkra mjukvaruplattformar. Ett exempel är att stödja svenska datacenter för att minska beroendet av amerikanska molntjänster.**
    - **Standardisering: Driv på för globala cybersäkerhetsstandarder inom EU och NATO, baserade på Sveriges höga krav, för att påverka leverantörers beteende.**
    - **Kritisk infrastruktur: Skydda fysisk och digital infrastruktur, som undervattenskablar, genom nationella säkerhetsprogram och internationella avtal.**
    - **Totalförsvarsintegration: Integrera cybersäkerhet fullt ut i Sveriges totalförsvar, med fokus på civil-militär samverkan och beredskap för hybridhot.**

NIS2:s långsiktiga påverkan

NIS2-direktivet är en språngbräda för Sveriges cybersäkerhetsambitioner. Genom att implementera dess krav – från säkerhetsåtgärder till internationellt samarbete – bygger Sverige en motståndskraft som kan stå emot dagens hot. Men direktivets verkliga värde ligger i dess potential att katalysera långsiktiga förändringar:

- **Konkurrenskraft: Företag som uppfyller NIS2:s krav kan positionera sig som pålitliga aktörer på den globala marknaden, vilket stärker Sveriges techsektor.**
- **Medborgarförtroende: En cybersäkerhet som respekterar integritet och transparens, som diskuterades i Kapitel 6, kan öka medborgarnas förtroende för staten och teknologin.**
- **Globalt ledarskap: Genom att gå bortom NIS2:s minimikrav kan Sverige inspirera andra länder och påverka internationella standarder.**

Men för att förverkliga denna potential måste Sverige övervinna de utmaningar som identifierats i tidigare kapitel: resursbrist, fragmentering och etiska dilemman. Detta

kräver politisk vilja, långsiktiga investeringar och en kultur där cybersäkerhet ses som en gemensam angelägenhet.

En fallstudie: Framtidens cyberförsvar

Tänk dig Sverige år 2035. En kvantdatorbaserad attack hotar att knäcka krypteringen i landets finanssystem. Men tack vare ett decennium av investeringar är Sverige förberett. Ett nationellt forskningscentrum har utvecklat kvantresistenta krypteringsmetoder, implementerade i banker och myndigheter. NCSC, nu med 200 anställda, koordinerar en snabb respons i samarbete med EU-CyCLONe och NATO. Kommuner, stärkta av statliga anslag, har robusta säkerhetssystem och utbildad personal. Medborgare, engagerade genom kampanjer som "Tänk säkert", rapporterar misstänkta aktiviteter i realtid.

Denna vision är inte orealistisk, men den kräver handling nu. Sverige måste prioritera cybersäkerhet som en nationell investering, precis som infrastruktur eller utbildning, för att undvika att bli en måltavla i en alltmer osäker värld.

Utmaningar på horisonten

Även med de bästa strategierna kommer Sverige att möta hinder:

- **Finansiering: Att finansiera forskning, utbildning och infrastruktur kräver betydande resurser, vilket kan vara svårt i en tid av ekonomiska utmaningar.**
- **Global konkurrens: Länder som USA, Kina och Israel investerar miljarder i cybersäkerhet. Sverige måste hitta sin nisch, som kvantkryptering eller 5G-säkerhet, för att konkurrera.**
- **Etiska frågor: Som diskuterades i Kapitel 6, måste Sverige fortsätta att balansera säkerhet med integritet för att behålla medborgarnas förtroende.**
- **Geopolitiska risker: Som Natomedlem och EU-land är Sverige exponerat för spänningar, särskilt i Östersjöregionen, vilket kräver en cybersäkerhet som är anpassad till hybridhot.**

Mot en global ledarroll

Sverige har alla förutsättningar att bli en global ledare inom cybersäkerhet: en högteknologisk ekonomi, en stark demokratisk tradition och en strategisk position i EU och NATO. NIS2 är startpunkten, men framtiden handlar om att bygga en cybersäkerhet som är proaktiv, innovativ och inkluderande. Genom att investera i människor, teknologi och samarbete kan Sverige inte bara skydda sig självt utan också visa världen hur säkerhet och frihet kan gå hand i hand.

I epilogen sammanfattar vi NIS2:s betydelse och utforskar hur Sverige kan fortsätta denna resa – inte bara som en implementerare av ett direktiv, utan som en pionjär i en digital era.

Epilog: Ett resilient Sverige

I en värld där osynliga hot kan lamslå samhällsviktiga tjänster på sekunder har NIS2-direktivet (Directive (EU) 2022/2555) blivit Sveriges kompass i en digital storm. Genom att införa strikta krav på säkerhetsåtgärder, snabb incidentrapportering och internationellt samarbete har direktivet byggt en grund för att skydda kritisk infrastruktur – från elnät och sjukhus till kommunala tjänster och datacenter. För Sverige, ett land vars välstånd och säkerhet är intimt kopplade till dess digitala ryggrad, är NIS2 inte bara en EU-förordning; det är en strategisk nödvändighet som stärker nationell motståndskraft i en tid av geopolitiska spänningar och teknologiska omvälvningar.

Denna bok har följt Sveriges resa med NIS2 – från dess tekniska detaljer och implementeringsutmaningar till dess etiska dilemman och framtida möjligheter. Vi har sett hur kommuner kämpar med resursbrist, hur näringslivet navigerar globala leverantörskedjor, och hur samarbete med EU och NATO formar Sveriges roll på den globala scenen. Men kanske viktigast har vi sett att cybersäkerhet är mer än teknik – det är en fråga om tillit, demokrati och samhällets förmåga att stå emot hot utan att kompromissa med sina värderingar.

NIS2:s betydelse för nationell säkerhet kan inte överskattas. Genom att tvinga fram robusta säkerhetsstandarder minskar direktivet risken för attacker som kunde störa vård, energi eller kommunikation. Genom att främja samarbete – nationellt och internationellt – bygger det en kollektiv motståndskraft som är större än summan av dess delar. Och genom att engagera medborgare, som i kampanjen "Tänk säkert", skapar det en kultur där säkerhet blir allas ansvar. Men denna resa är långt ifrån över. NIS2 är en början, inte ett slut.

Därför är detta en uppmaning till fortsatt engagemang. Till regeringen: Investera i utbildning, forskning och nationell kapacitet för att möta framtida hot som kvantdatorer och AI-drivna attacker. Till näringslivet: Se cybersäkerhet som en konkurrensfördel, inte en börda, och samarbeta för att säkra leverantörskedjor och innovationer. Och till medborgarna: Ta ansvar för er digitala säkerhet – ett starkt

lösenord, en misstänksamhet mot phishing-mejl, eller en rapport om en misstänkt incident kan göra skillnad. Tillsammans kan vi bygga ett Sverige som inte bara överlever cyberhot, utan blomstrar i deras skugga.

Cybersäkerhet är mer än ett skydd mot angrepp – det är en grund för demokrati och välstånd. Ett samhälle som kan lita på sina digitala system är ett samhälle där medborgare kan rösta utan rädsla för manipulation, där företag kan innovera utan risk för spionage, och där välfärdstjänster kan levereras utan avbrott. Sverige, med sin tradition av transparens, innovation och samarbete, har alla förutsättningar att leda denna utveckling. Genom att omfamna NIS2 och gå bortom dess krav kan vi visa världen att säkerhet och frihet inte är motsatser, utan två sidor av samma mynt.

Låt oss ta detta tillfälle. Låt oss bygga ett resilient Sverige – inte bara för idag, utan för generationer framöver.

Bilagor

Ordlista

This glossary defines key technical terms used throughout the book to ensure clarity for readers, from policymakers to general audiences. Terms are explained in a straightforward manner, avoiding overly technical language while retaining accuracy.

- **CSIRT (Computer Security Incident Response Team): En grupp eller organisation som ansvarar för att hantera och mildra cyberincidenter, såsom dataintrång eller attacker. I Sverige är MSB:s CSIRT en central aktör som koordinerar responsen på nationell nivå och samarbetar med internationella CSIRT-nätverk under NIS2.**
- **DDoS (Distributed Denial-of-Service): En typ av cyberattack där angripare överbelastar en webbplats eller tjänst med trafik från flera källor, vilket gör den otillgänglig. Exempelvis drabbades svenska banker av DDoS-attacker 2024.**
- **Kryptering: En process för att skydda data genom att omvandla dem till en oläslig form som endast kan dekrypteras med rätt nyckel. NIS2 kräver att organisationer använder kryptering för att säkra känslig information.**
- **Multifaktorautentisering (MFA): En säkerhetsåtgärd som kräver minst två former av verifiering (t.ex. lösenord och en kod från en mobilapp) för att logga in. NIS2 uppmuntrar MFA för att skydda system.**

- **Nolldagsexploatering: En attack som utnyttjar en okänd sårbarhet i mjukvara innan utvecklaren har haft chans att åtgärda den. Sådana attacker är särskilt farliga och svåra att försvara sig mot.**
- **Phishing: En metod där angripare skickar falska e-postmeddelanden eller meddelanden som ser legitima ut för att lura användare att lämna ut inloggningsuppgifter eller klicka på skadliga länkar. Phishing är en vanlig ingångspunkt för attacker.**
- **Ransomware: En typ av skadlig kod som låser en organisations system eller data och kräver en lösensumma för att låsa upp dem. Svenska kommuner har drabbats hårt av ransomware, med kostnader i miljontals kronor.**
- **SCADA (Supervisory Control and Data Acquisition): System som används för att övervaka och styra industriella processer, som elnät eller vattenverk. SCADA-system är ofta mål för cyberattacker på grund av deras kritiska roll.**
- **Spearphishing: En riktad form av phishing där angripare skräddarsyr meddelanden för specifika individer eller organisationer, ofta baserat på insamlad information, för att öka chansen till framgång.**
- **Tredjepartsleverantör: Ett företag eller organisation som tillhandahåller tjänster eller produkter till en annan organisation, som molntjänster eller mjukvara. NIS2 kräver att tredjepartsleverantörer säkras som en del av leverantörskedjan.**

Tidslinje

This timeline highlights key events in the development of the NIS2 Directive and Sweden's cybersecurity efforts, providing historical context for the book's narrative. It focuses on milestones from the adoption of NIS1 to the anticipated full implementation of NIS2.

- **2016: EU antar NIS1-direktivet (Directive (EU) 2016/1148), det första ramverket för att harmonisera cybersäkerhet i medlemsstaterna. Sverige införlivar direktivet i nationell lagstiftning genom ändringar i säkerhetsskyddslagen.**
- **2018: Sverige implementerar NIS1 fullt ut, med MSB som samordnande myndighet. Kommuner och vissa sektorer rapporterar dock brister i resurser för att uppfylla kraven.**
- **2020: EU-kommissionen identifierar brister i NIS1, såsom ojämn implementering och begränsat tillämpningsområde. Arbetet med NIS2 påbörjas som en del av EU:s cybersäkerhetsstrategi.**

- **2021: Nationellt cybersäkerhetscenter (NCSC) etableras i Sverige, samlande expertis från MSB, Försvarsmakten, Säkerhetspolisen och FRA för att stärka hotanalys och incidenthantering.**
- **2022 (december): NIS2-direktivet antas av EU-parlamentet och rådet, med målet att stärka cybersäkerheten för samhällsviktiga tjänster och harmonisera regler.**
- **2023 (januari): NIS2 träder i kraft. Medlemsstater, inklusive Sverige, ges till oktober 2024 för att införliva direktivet i nationell lagstiftning.**
- **2023: Sverige lanserar kampanjen "Tänk säkert" för att öka medborgares och småföretags medvetenhet om cybersäkerhet, finansierad med 50 miljoner kronor.**
- **2024 (tidigt): Utredningen *Cybersäkerhet i samhällsviktiga tjänster* (SOU 2024:47) presenteras, med förslag på hur NIS2 ska integreras i svensk lag, inklusive ändringar i säkerhetsskyddslagen.**
- **2024 (oktober): Undervattenskablar i Östersjön skadas under misstänkta omständigheter, vilket understryker vikten av leverantörskedjesäkerhet och kritisk infrastruktur i NIS2.**
- **2025 (våren, förväntat): Ett lagförslag baserat på SOU 2024:47 läggs fram i riksdagen, med målet att träda i kraft senast oktober 2025.**
- **2025: Sverige avsätter 196 miljoner kronor i budgeten för cybersäkerhet, inklusive stöd till NCSC, kommuner och "Tänk säkert"-kampanjen.**
- **2026 (förväntat): Full implementering av NIS2 i Sverige, med tillsyn av MSB och sektorsspecifika myndigheter. Organisationer förväntas ha anpassat sig till direktivets krav.**

Referenser

This reference list includes key sources cited or consulted in the book, providing credibility and resources for further reading. It focuses on official documents, reports, and authoritative publications relevant to NIS2 and Sweden's cybersecurity.

- **EU-dokument:**
  - **Directive (EU) 2016/1148 (NIS1). *Official Journal of the European Union*, L 194, 19 July 2016. Hämtad från: https://eur-lex.europa.eu/eli/dir/2016/1148/oj**
  - **Directive (EU) 2022/2555 (NIS2). *Official Journal of the European Union*, L 333, 27 December 2022. Hämtad från: https://eur-lex.europa.eu/eli/dir/2022/2555/oj**

    - **European Commission. (2020). *EU Cybersecurity Strategy for the Digital Decade*. Hämtad från: https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade**
- **Svenska myndighetsrapporter:**
    - **Myndigheten för samhällsskydd och beredskap (MSB). (2024). *Cybersäkerhetsläget i Sverige 2024*. Hämtad från: https://www.msb.se**
    - **Säkerhetspolisen. (2024). *Årsbok 2024*. Hämtad från: https://www.sakerhetspolisen.se**
    - **Försvarets radioanstalt (FRA). (2024). *Cyberhot mot Sverige: En analys av trender och risker*. Hämtad från: https://www.fra.se**
    - **Statens offentliga utredningar. (2024). *Cybersäkerhet i samhällsviktiga tjänster* (SOU 2024:47). Hämtad från: https://www.regeringen.se**
- **Övriga källor:**
    - **Svenskt Näringsliv. (2024). *Företagens beredskap för NIS2: En undersökning*. Hämtad från: https://www.svensktnaringsliv.se**
    - **Nationellt cybersäkerhetscenter (NCSC). (2024). *Årsrapport 2024: Hot och incidenter*. Hämtad från: https://www.ncsc.se**
    - **Post- och telestyrelsen (PTS). (2023). *5G-säkerhet i Sverige: Utmaningar och lösningar*. Hämtad från: https://www.pts.se**